ARES Conference

International Conference on Availability, Reliability and Security

University College Dublin, Dublin, Ireland
August 25 – August 28, 2020

“DIDEROT

An Intrusion Detection and Prevention System for DNP3-based SCADA Systems

Panagiotis Radoglou-Grammatikis

University of Western Macedonia

psarigiannidis@uowm.gr

Co-Authors

SDN-µSense

ARES Conference
International Conference on Availability, Reliability and Security

University of Western Macedonia

Panagiotis Radoglou-Grammatikis
Panagiotis Sarigiannidis

0Infinity Limited

George Efstathopoulos

Sidroco Holdings

Paris-Alexandros Karypidis
Antonios Sarigiannidis

Introduction

- In the era of hyper-connected digital economies, the smart technologies play a vital role in the operation of the electrical grid, transforming it into a new.
- This new reality introduces severe cybersecurity issues due to insecure, legacy protocols.
- This paper presents an ML-based IDPS called DIDEROT which is capable of detecting cyberattacks and anomalies against DNP3.

DIDEROT Contributions

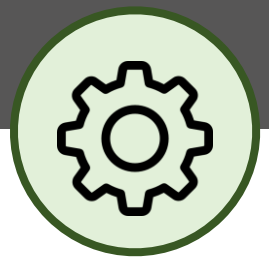
DIDEROT relies on network flow statistics, including two detection layers: a) intrusion detection and b) anomaly detection. Intrusion Detection relies on supervised ML detection methods and is responsible for recognising particular DNP3 cyberattacks: a) injection, b) flooding, c) DNP3 reconnaissance, d) replay attacks and e) masquerading. Anomaly detection is activated when the first layer classifies a network flow as normal. Thus, the second layer undertakes to identify whether a DNP3 anomaly takes place either due to a security violation or a possible electricity disturbance. To this end, the DIDEROT autoencoder was developed. DIDEROT takes full advantage of SDN in order to mitigate the DNP3 cyberattacks/anomalies.

Detecting DNP3 cyberattacks

DIDEROT can detect a plethora of DNP3 cyberattacks by using supervised ML detection methods and particularly a decision tree classifier.

Detecting DNP3 anomalies

DIDEROT can recognise DNP3 anomalies that take place either due to a security violation or an electricity disturbance. An autoencoder Deep Neural Network (DNN) was developed for this purpose called DIDEROT Autoencoder



ML Methods Evaluation

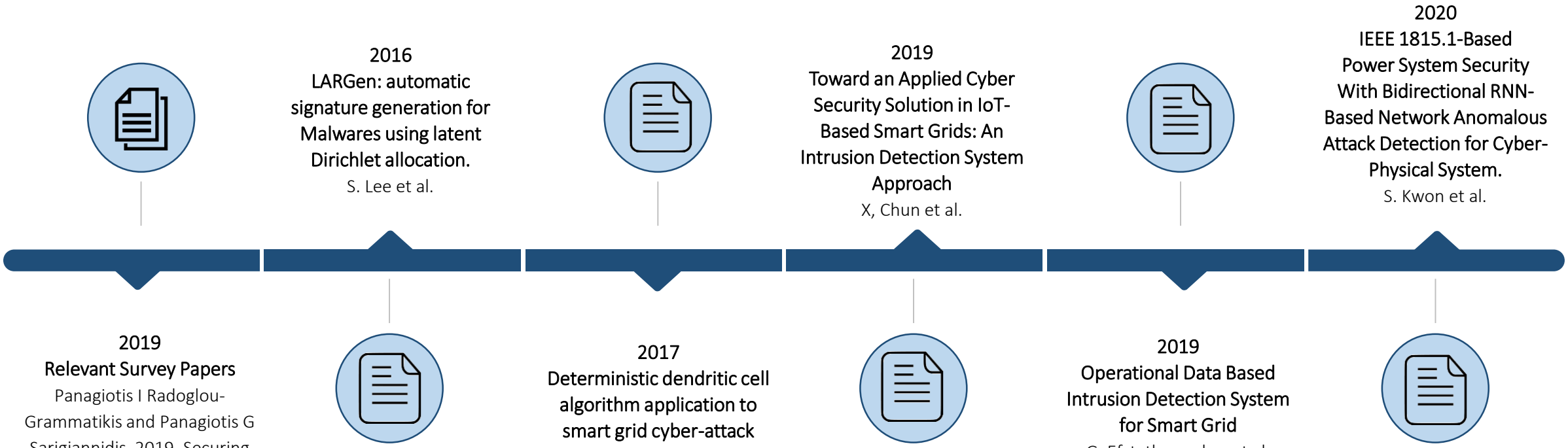
Various ML methods were assessed, using real DNP3 netdatawork traffic originating from a substation environment

Mitigating DNP3 cyberattacks/anomalies

Based on the DIDEROT detection results, DIDEROT takes full advantage of SDN in order to mitigate timely the DNP3 cyberattacks and anomalies.

Related Work

IDPS for Smart grid and DNP3 SCADA Systems



Background

- **DNP3 SCADA Systems**: Overview of DNP3 and relevant attacks
- **Typical IDPS Architecture**: Main components of a typical IDPS system.
- **Detection Techniques**: Overview of the detection techniques
- **ML Detection**: Overview of ML-based detection methods.

DNP3 SCADA Systems

Injection

The cyberattacker injects malicious DNP3 packets.

Flooding

DNP3 DoS, where the cyberattacker floods the target with multiple DNP3 packets

DNP3 Reconnaissance

It refers to DNP3 packets sent to the target system to identify whether it uses DNP3 or not.

Replay

It captures legitimate DNP3 packets and re-transmit them after a specific delay.

Masquerading

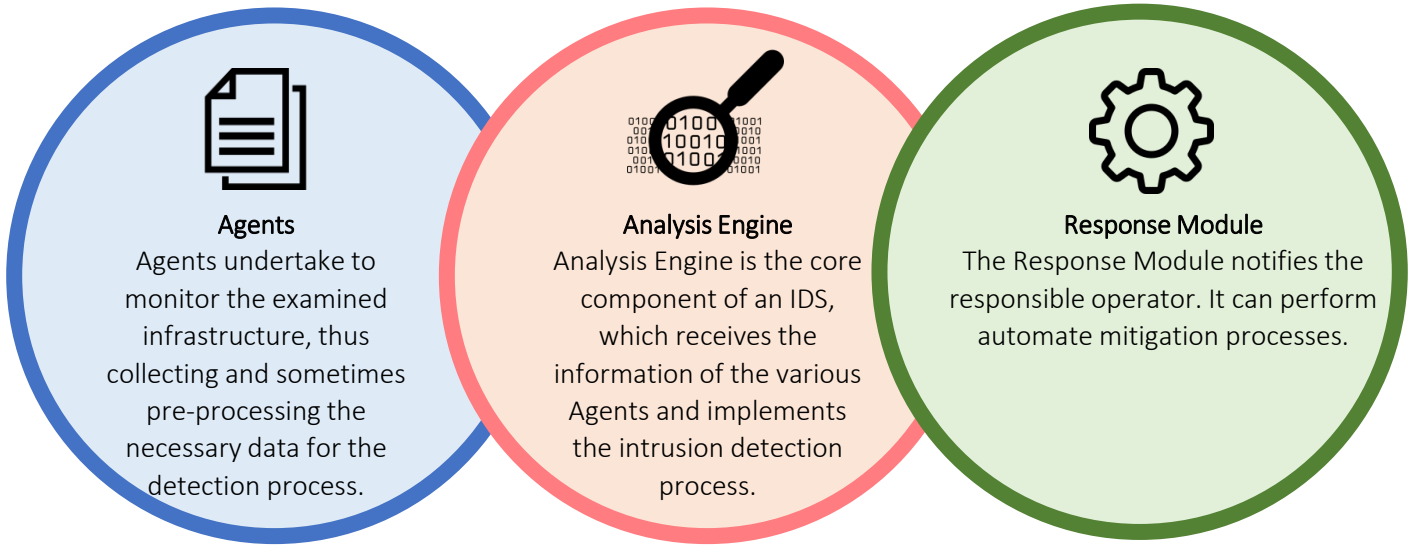
Impersonates the DNP3 behaviour of the legitimate asset

DNP3 PROTOCOL

DNP3 is a reliable protocol adopted in Critical Infrastructures, mainly in the US. In a SCADA system, DNP3 is used to exchange messages between a master (i.e., MTU) and outstation or differently slave (i.e., PLC or RTU). Several topologies: a) point-to-point, b) multiple-drop and c) hierarchical. Three layers: y, a) link layer, b) transport layer and c) application layer. DNP3 can operate over TCP/IP where all DNP3 layers are incorporated into the application layer of TCP/IP

Typical IDPS Architecture

Three Main Components



Based on the RFC 2828, intrusion detection is defined as the process aiming to audit and investigate security events in order to recognise a possible security policy violation. In 1980, the IDS term was introduced as a hardware or software system capable of automating the intrusion detection process. In particular, in 1980, J. Anderson highlighted the significance of the log files during an intrusion detection procedure. Another remarkable case is the paper of D. Denning, who defined a theoretical IDS model based on abstract feature patterns. According to D. Denning, if a system cannot operate based on its specifications, then it has been probably affected by a threat.

Detection Techniques

1

SIGNATURE-BASED DETECTION

The signature-based detection defines specific rules called signatures that reflect malicious patterns. If the characteristics of the monitoring data match with those of the signatures, then a possible security violation takes place.

2

ANOMALY-BASED DETECTION

The anomaly-based detection applies statistical analysis and Artificial Intelligence (AI) methods.

3

SPECIFICATION-BASED DETECTION

The specification-based detection defines a set of rules called now specifications that define the normal operation of the monitored system/infrastructure. If the characteristics of the monitored data do not agree with those of the specifications, then a security violation is carried out.

ML Detection

Three Main Steps

Preprocessing

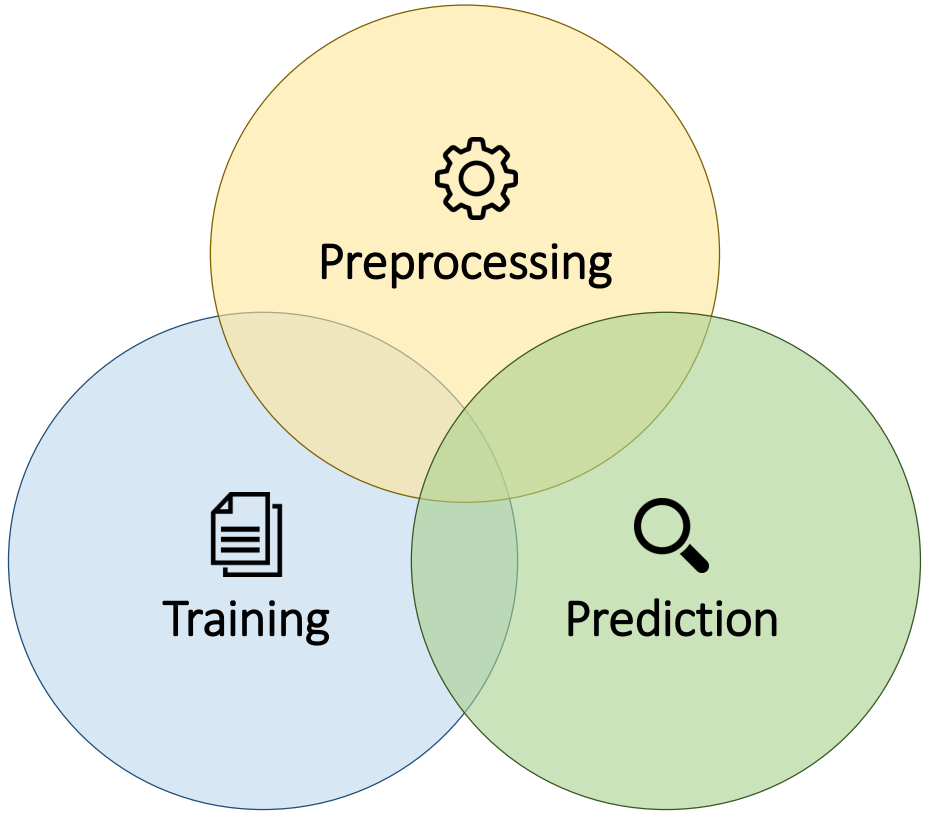
Processes appropriately the input data so that it will be in accordance with the corresponding ML model. Usually, data-preprocessing methods are applied, such as min-max scaling, normalisation, standardisation, robust scaler and max abs scaler

Training

Supervised detection methods, unsupervised/oulier detection methods and semi-supervised/novelty detection methods

Prediction

The ML model can be deployed in order to predict unknown data after the execution of the same pre-processing tasks of the first phase



DIDEROT

- **DIDEROT Architecture**: a) Data Monitoring Module, b) DIDEROT Analysis Engine, c) Response Module
- **DIDEROT Autoencoder**: capable of detecting DNP3 anomalies
- **DIDEROT Evaluation**: Evaluation Environment, Dataset, Comparison with other ML models

DIDEROT Architecture

Thee Main Components

Data Monitoring Module

It monitors the network traffic and feeds the DIDEROT Analysis Engine with network flows statistics. **Tools**: Tshark, CICFlowMeter.

Preprocessing: Min_Max Scaler. $z = \frac{x - \min(x)}{\max(x) - \min(x)}$

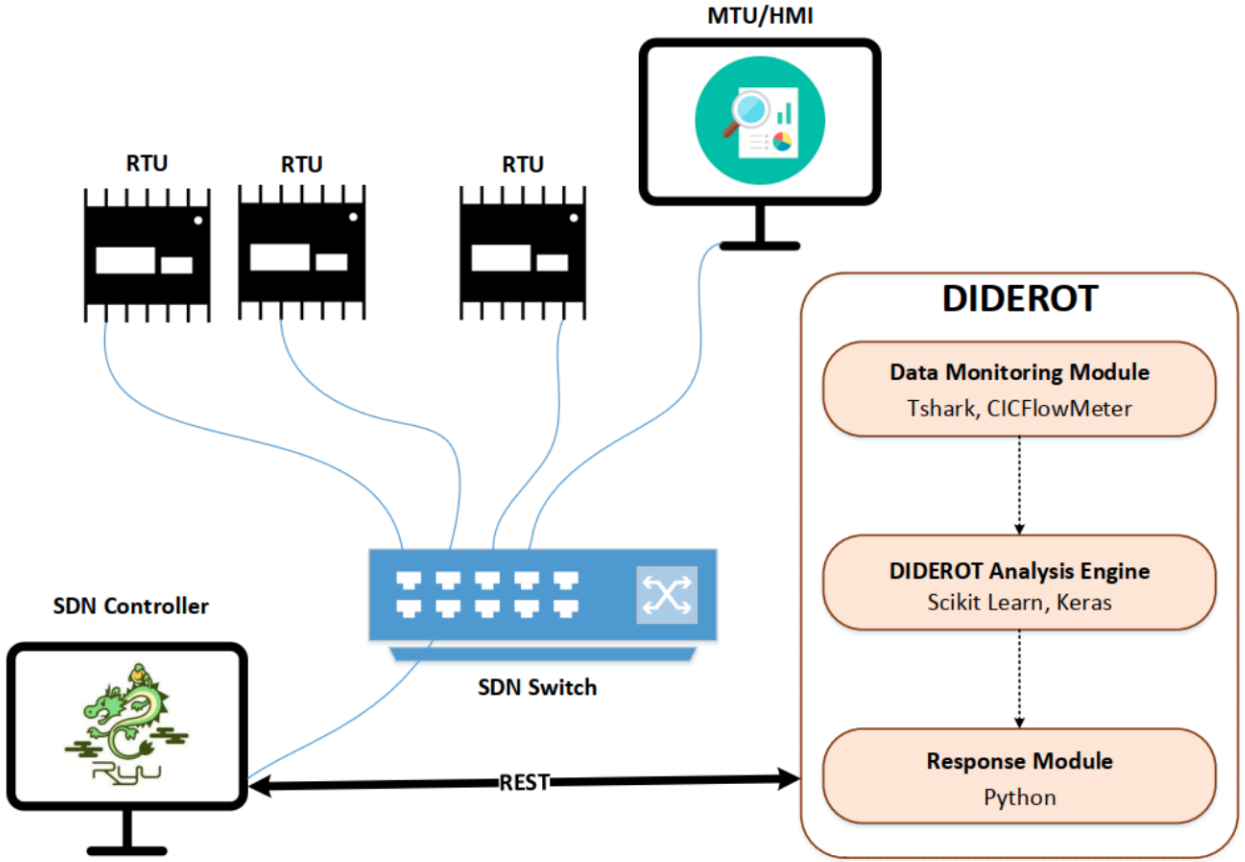
DIDEROT Analysis Engine

First Detection Layer - Intrusion Detection: Decision Tree Classifier. Multiclass Classification (Injection, Flooding, DNP3 Reconnaissance, Replay, Masquerading)

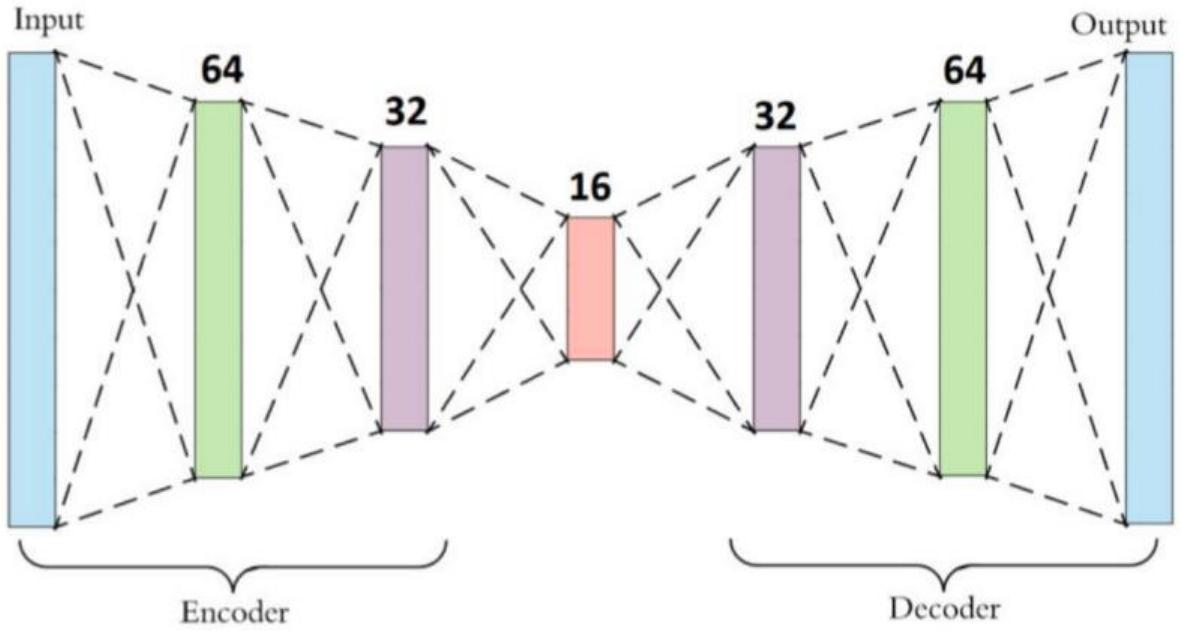
Second Detection Layer - Anomaly Detection: DIDEROT Autonecoder

Response Module

Security Events based on the AlienVault OSSIM format; It informs the SDN Controller (Ryu) to drop the malicious DNP3 flows



DIDEROT Autoencoder



DIDERROT Autoencoder maps input data $x \in X = \mathbb{R}^n$ to an output $x' \in X$. It consists of an encoder $f : X \rightarrow Z$ and a decoder $g : Z \rightarrow X$, each implemented as a deep neural network. The encoder and decoder together result the output $x' = g(f(x))$.

The low-dimensional latent representation of x is obtained from the encoder and is defined as $z = f(x) \in Z = R^m$ $(m << n)$. DIDERROT Autoencoder avoids to become an identity function and the training process aims to minimise the reconstruction error $L(x, x')$.

Anomalies are detected by measuring the reconstruction error $L(x,x')$ and comparing it with a threshold T, classifying all operational data samples y with $L(y, g(f(y))) > T$ as anomalies. T is estimated heuristically based on the reconstruction error L of all normal training data samples. The threshold T in order to be more robust is selected to be a large percentile of the reconstruction error $T = p0.9(L(x, x')| \; x \in X)$ or if a validation dataset is available is selected to maximise the performance for the validation data.

DIDEROT Evaluation

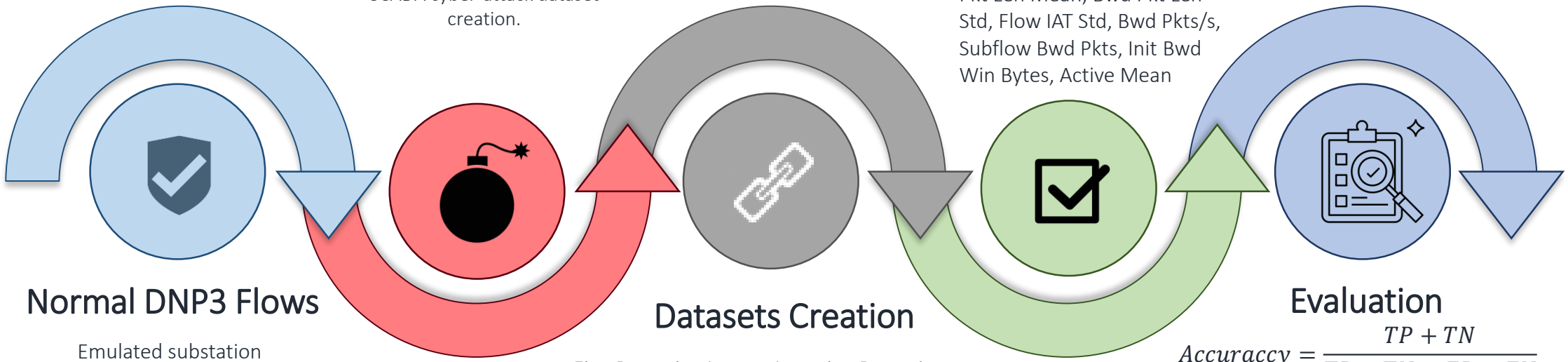
Evaluation Flow

Malicious DNP3 Flows

N. Rodofile et al. Framework for SCADA cyber-attack dataset creation.

Feature Selection

Flow Duration, TotLen Fwd Pkts, Fwd Pkt Len Mean. Fwd Pkt Len Mean, Bwd Pkt Len Std, Flow IAT Std, Bwd Pkts/s, Subflow Bwd Pkts, Init Bwd Win Bytes, Active Mean



Normal DNP3 Flows

Emulated substation environment equipped with real industrial devices such as RTUs, IEDs. Via SPAN, the Data Monitoring Module can receive the overall DNP3 traffic, extracting the normal network flow statistics.

Datasets Creation

First Detection Layer – Intrusion Detection: Balanced, labelled dataset composed of both normal and DNP3 cyberattack flows

Second Detection Layer – Anomaly Detection: The training dataset includes only normal flows. The testing dataset includes both normal and abnormal flows. The labels of the abnormal flows are characterized as “Anomaly”

Evaluation

$$Accuraccy = \frac{TP + TN}{TP + TN + FP + FN}$$

$$TPR = \frac{TP}{TP + FN}$$

$$FPR = \frac{FP}{FP + TN}$$

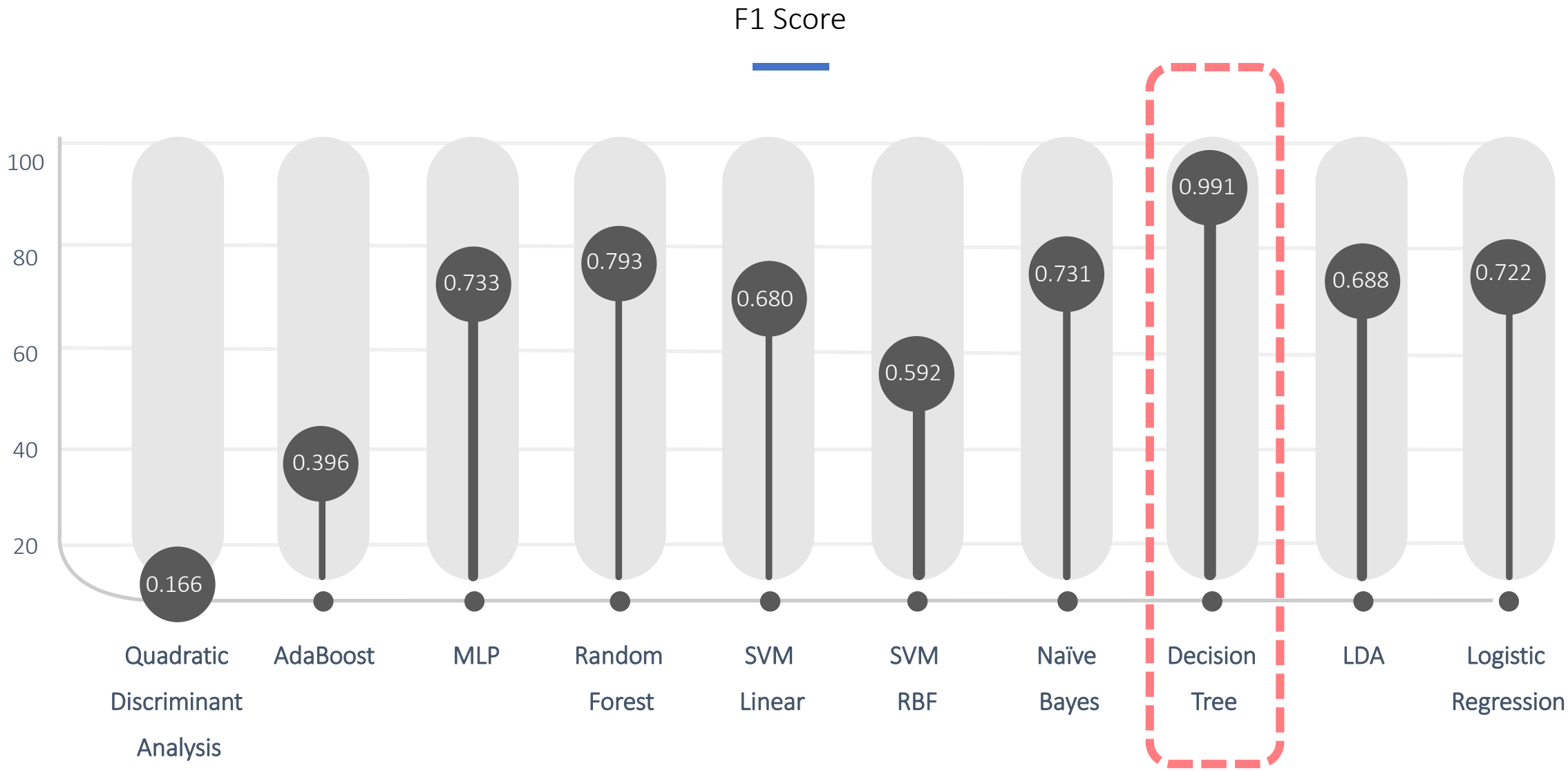
$$F1 = \frac{2 \times Precision \times TPR}{Precision + TPR} \text{ where } Precision = \frac{TP}{TP + FP}$$

First DIDEROT Detection Layer – Intrusion Detection

First DIDEROT Detection Layer – Intrusion Detection

First DIDEROT Detection Layer – Intrusion Detection

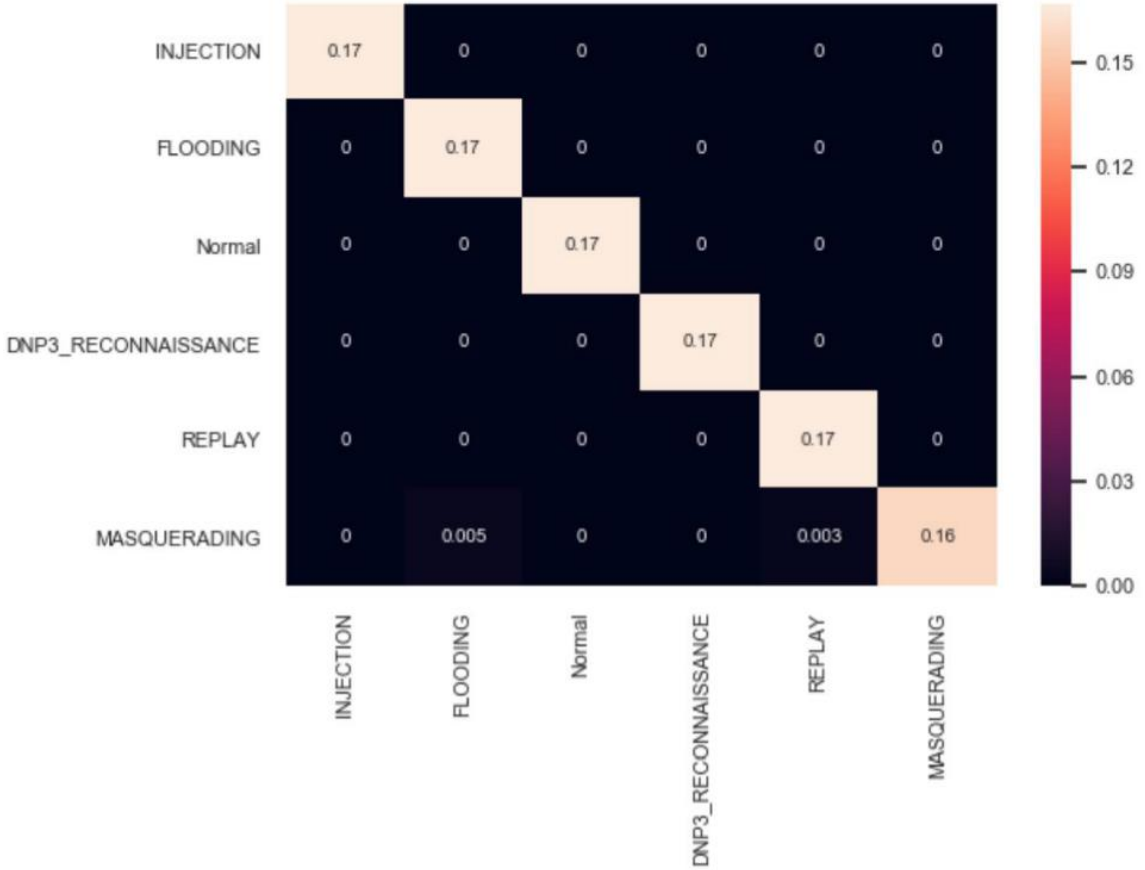
First DIDEROT Detection Layer – Intrusion Detection



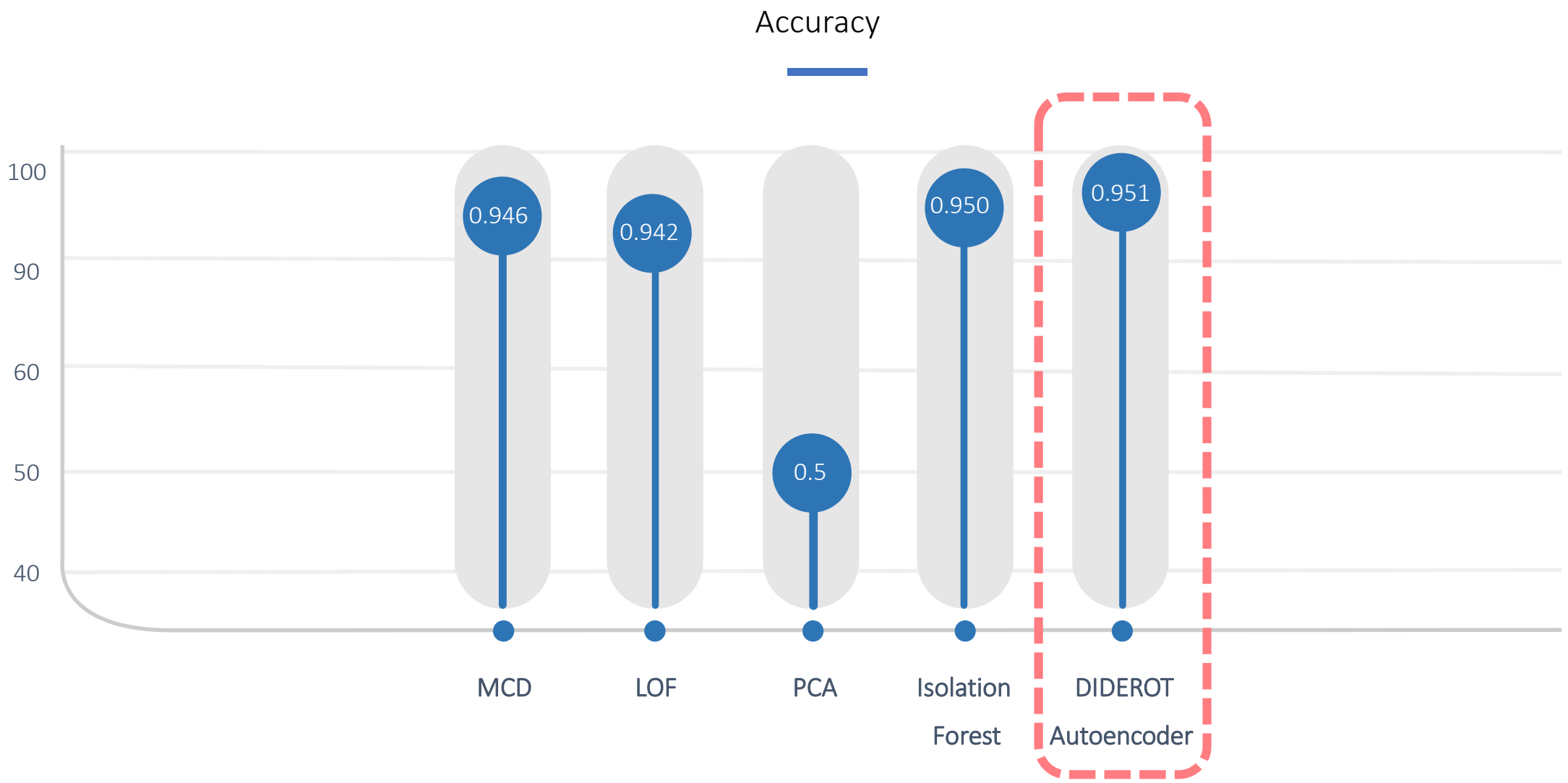
First DIDEROT Detection Layer – Intrusion Detection

Aggregate Comparative Results

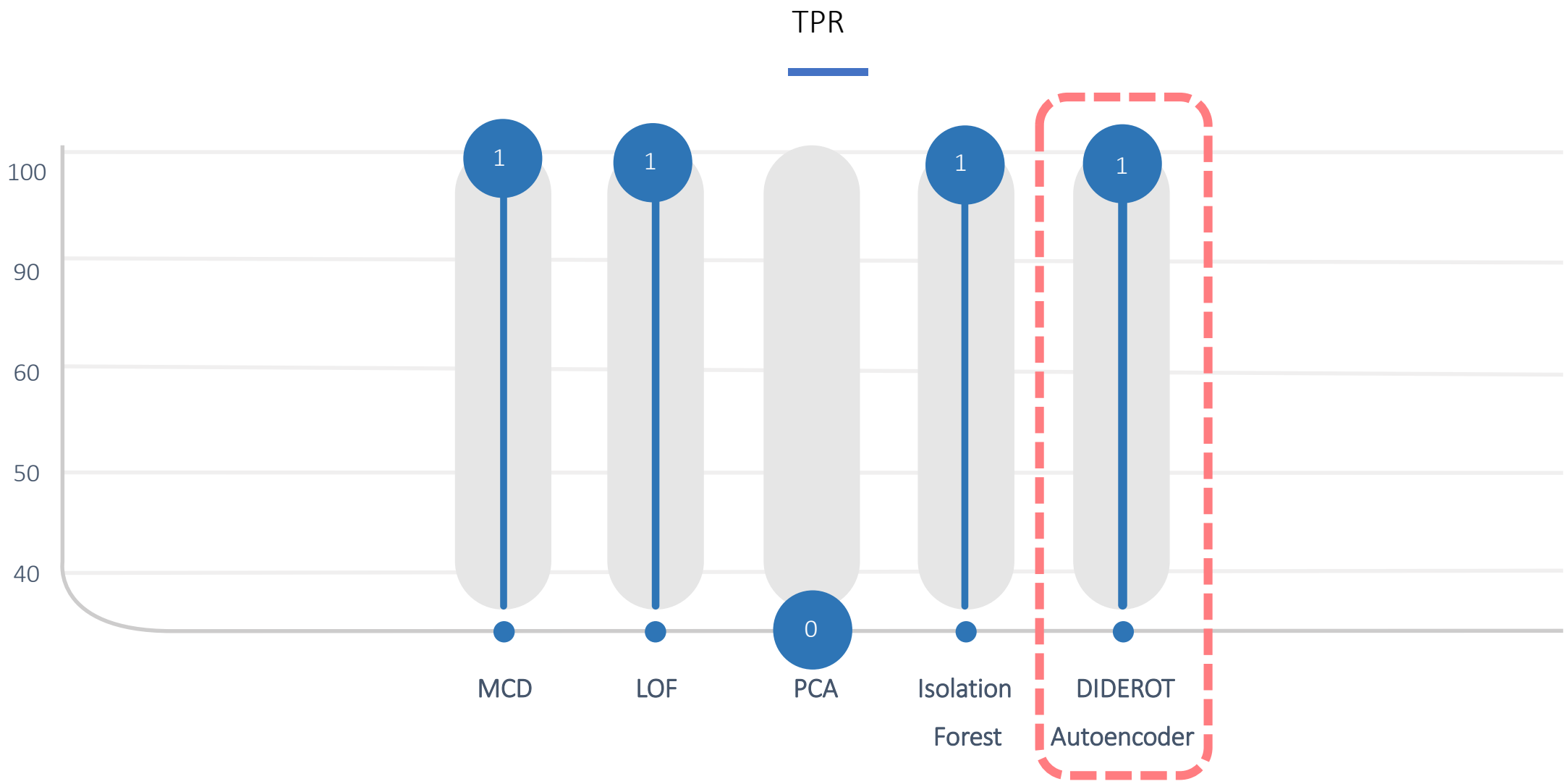
ML Method	Accuracy	TPR	FPR	F1
Quadratic Discriminant Analysis	0.722	0.166	0.166	0.166
AdaBoost	0.798	0.396	0.120	0.396
MLP	0.911	0.733	0.053	0.733
Random Forest	0.931	0.793	0.041	0.793
SVM Linear	0.893	0.680	0.063	0.680
SVM RBF	0.864	0.592	0.081	0.592
Naive Bayes	0.910	0.731	0.053	0.731
Decision Tree	**0.997**	**0.991**	**0.001**	**0.991**
LDA	0.896	0.688	0.062	0.688
Logistic Regression	0.907	0.722	0.055	0.722



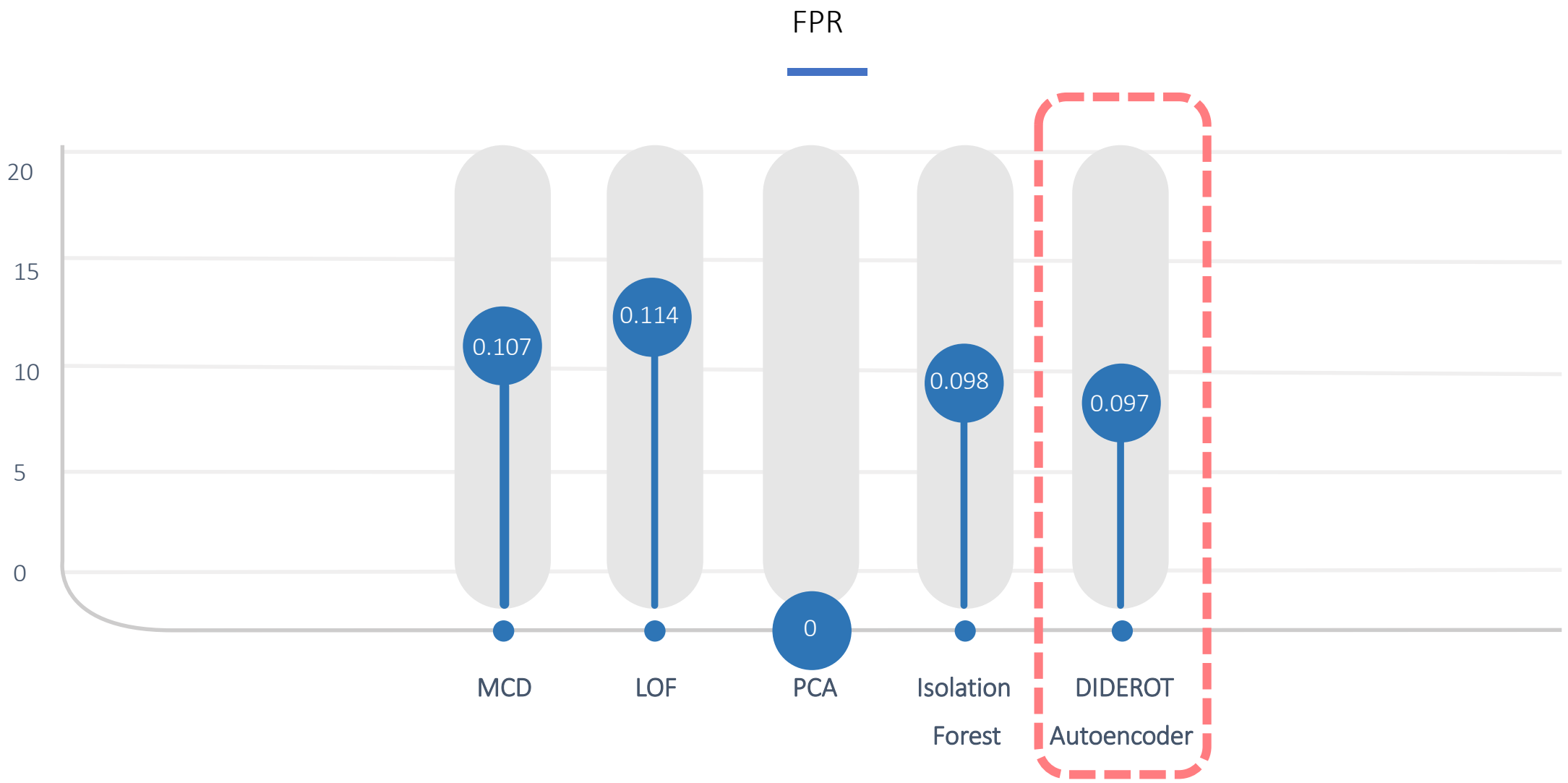
Second DIDEROT Detection Layer – Anomaly Detection



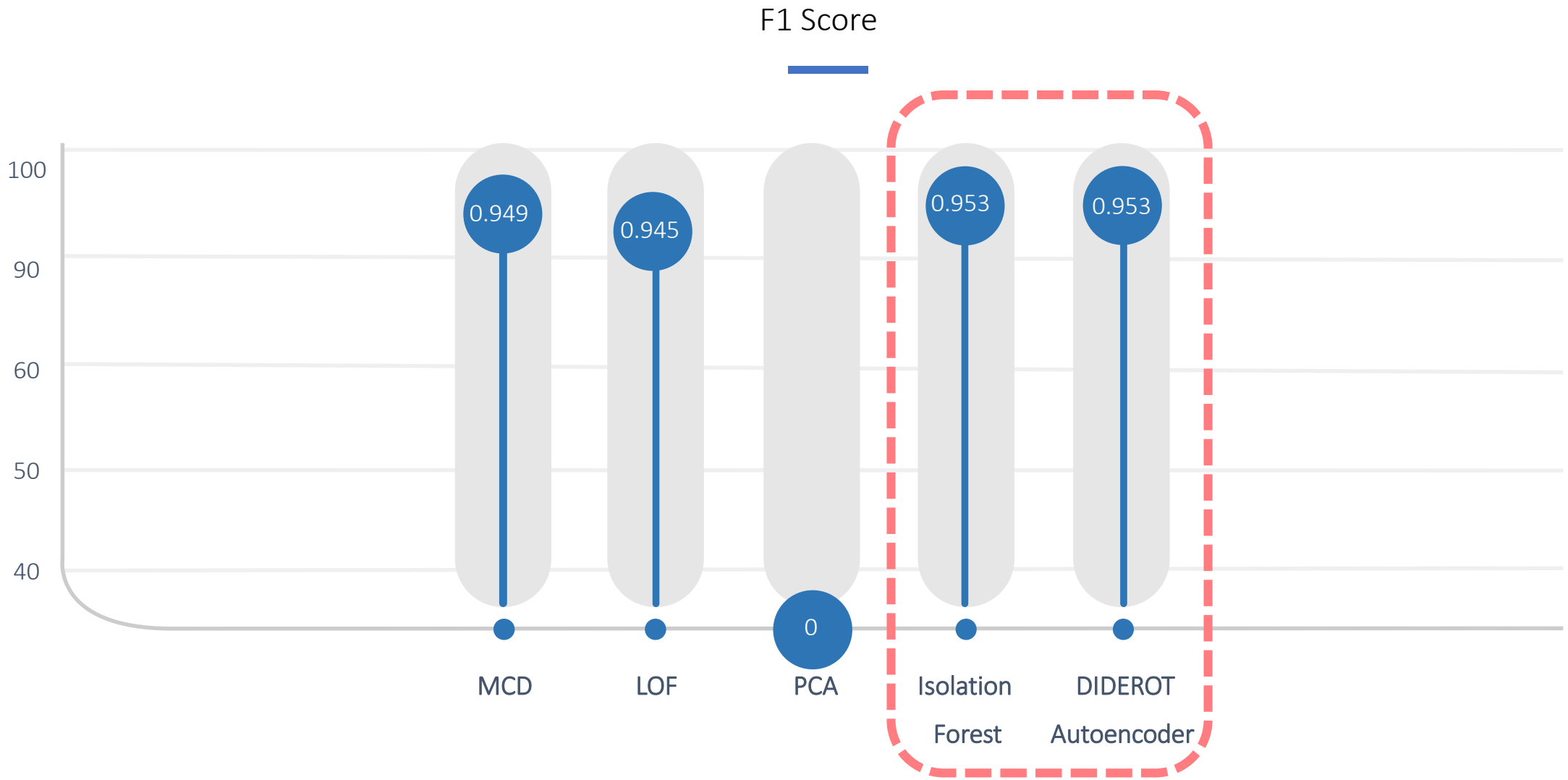
Second DIDEROT Detection Layer – Anomaly Detection



Second DIDEROT Detection Layer – Anomaly Detection



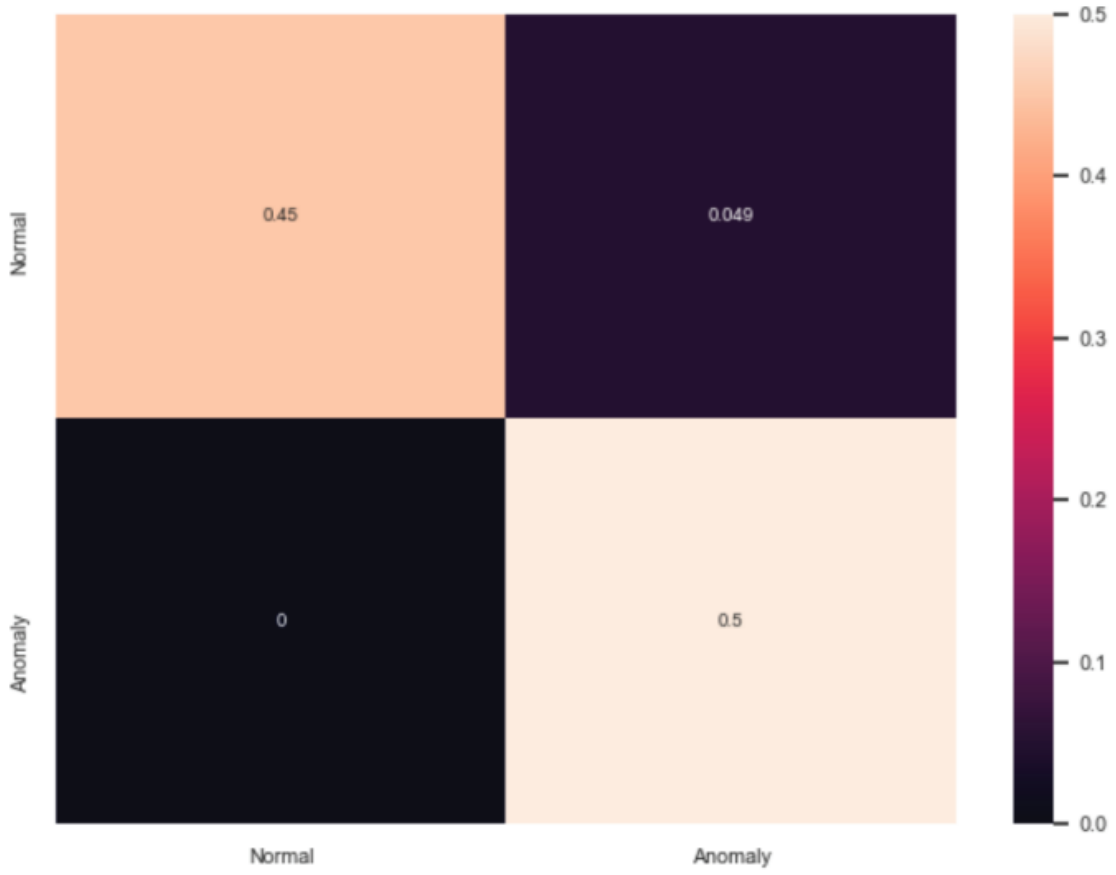
Second DIDEROT Detection Layer – Anomaly Detection



Second DIDEROT Detection Layer – Anomaly Detection

Aggregate Comparative Results

ML Method	Accuracy	TPR	FPR	F1
MCD	0.946	1	0.107	0.949
LOF	0.942	1	0.114	0.945
PCA	0.5	0	0	0
Isolation Forest	0.950	1	0.098	0.953
DIDEROT Autoencoder	**0.951**	**1**	**0.097**	**0.953**



Conclusions

The technological leap of the smart grid demands appropriate security measures. The presence of timely and accurate IDPS is necessary.

In this paper, we presented an IDPS for the DNP3 protocol called DIDEROT. DIDEROT relies on ML-based detection techniques, thus detecting DNP3 attacks and anomalies

Future Plans: Association rules that will combine the two detection layers of DIDEROT; intrusion detection mechanisms for other industrial protocols, such as Profinet, EtherCAT and IEC 60870-5-104

Thank You & Q/A

Contact us

pradoglou@uowm.gr

http://www.sdnmicrosense.eu/

https://gr.linkedin.com/in/panagiotisrg

https://www.youtube.com/channel/UC5xpUNpQQ6eAQvc5JpnWWGw

Thank You

Questions ?